Vastine artikkeliin ”GDPR ei toimi – Tietosuojakäytännöt eivät noudata asetusta”

JYRI PAASONEN & JYRKI MANNELIN

Valtteri Sankari ja Matti Wiberg kirjoittivat *Yhteiskuntapolitiikka*-lehteen 3/19 artikkelin ”GDPR ei toimi – Tietosuojakäytännöt eivät noudata asetusta”. Artikkelissaan he ansiokkaasti kuvaavat näkemystään tietosuojan nykytilasta Suomessa perustellen päätelmiään tekemällään tutkimuksella, jossa he sovelsivat toimintatutkimuksen tekniikoita. Pääasiallinen aineistonkeruumetodi oli havainnointi. Kohteet valittiin julkiselta ja yksityiseltä sektorilta. He kävivät 11 kohteessa ja sähköisiä yhteydenottoja oli kahdeksan.

Tutkimuksensa päätelmänä he toteavat EU:n tietosuoja-asetuksen säännösten jäävän Suomessa noudattamatta rekisteröidyn suostumuksen osalta ja rekisteröidyn suostumuksen olevan suureksi osaksi illuusio. Lisäksi he toteavat rekisterinpitäjillä olevan tarvetta kouluttaa henkilöstöään ja valvoa näiden tekemisiä nykyistä paremmin. He toteavat myös valvontaviranomaisen laiminlyöneen velvollisuutensa suurilta osin ja nostavat esille mahdollisen tarpeen kansallisen lainsäädännön tarkentamiselle.

Yhdymme edellä esitetyistä väitteistä siihen, että rekisterinpitäjien tulee nykyistä paremmin tunnistaa EU:n tietosuoja-asetuksessa määritellyt velvollisuutensa, tiedostaa henkilötietojen rekisteröintiperusteet, kouluttaa henkilöstöään paremmin henkilötietojen käsittelyn osalta ja valvoa näiden lainmukaista toimintaa nykyistä paremmin. Emme kuitenkaan yhdy kaikkiin kirjoittajien näkemyksiin tietosuojasta ja tietosuoja-asetuksen soveltamisesta. Lisäksi tässä kirjoituksessa korjataan Sankarin ja Wibergin osittain virheellisiä tulkintoja lainsäädännöstä.

EU:n tietosuoja-asetuksen soveltamisalue

Sankarin ja Wibergin artikkelissa kuvattu tutkimus kohdistuu osittain sellaisiin EU:n ja ETA:n ulkopuolella sijaitseviin yrityksiin, joilla ei ole velvollisuutta noudattaa EU:n tietosuoja-asetuksessa säädettyjä henkilötietojen käsittelyperusteita ja jotka eivät ole ilmoittaneet noudattavansa ko. sääntelyä vapaaehtoisesti. Artikkelissa esitetyt johtopäätökset näiden toimijoiden EU:n tietosuoja-asetuksen noudattamisesta tai noudattamatta jättämisestä ovat vailla oikeusperustetta.

EU:n ja ETA:n ulkopuolelle pääkonttorinsa (rekisteröimismaa) sijoittaneet yritykset eivät ole velvoitettuja noudattamaan EU:n lainsäädäntöä, vaan ne noudattavat oman valtionsa voimassa olevaa lainsäädäntöä, jonka henkilötietojen käsittelyyn liittyvät säännökset voivat poiketa merkittävästi EU:n säännöksistä.

Osa EU:n ja ETA:n ulkopuolelle sijoittuneista yrityksistä on kuitenkin katsonut omien intressiensä perusteella tarpeelliseksi noudattaa EU:n tietosuoja-asetusta riippumatta pääkonttorinsa rekisteröimismaasta. Tällaiset yritykset ovat yleensä itse vapaaehtoisesti julkaisseet yksiselitteisen tiedon EU:n tietosuoja-asetuksen noudattamisesta.

Henkilötietojen käsittelyperusteet

Suostumuksen vaatimus. Sankarin ja Wibergin artikkelissa lähtökohtaisesti painotetaan henkilön suostumusta ainoana perusteena henkilötietojen lailliselle käsittelylle. Tämä siitä huolimatta, että artikkelissa todetaan EU:n tietosuoja-asetuksessa olevan useita perusteita henkilötietojen lailliselle käsittelylle.

Käyttämällä suostumusta lähtökohtana Sankarin ja Wibergin tutkimuksessa käytiin neljässä kohteessa esittäytymällä uudeksi asiakkaaksi ja seitsemässä nykyi-

senä asiakkaana. Kohteissa selvitettiin, onko suostumus annettu, ja jos on, niin miten, milloin ja mihin tarkoitukseen. Lisäksi kysyttiin yleisesti tietosuojasta ja henkilötietojen käsittelystä.

Sankari ja Wibergi lähtevät sivuraiteille heti lähtökohdiltaan, koska he jättävät huomioimatta EU:n tietosuoja-asetuksessa säädetyt muut lailliset henkilötietojen käsittelyperusteet, jotka asiakassuhteessa perustuvat sopimussuhteeseen ja viranomaistoiminnassa julkisen vallan käyttöön eivätkä suinkaan rekisteröidyn antamaan yksiselitteiseen, vapaaehtoiseen, yksilöityyn ja tietoiseen suostumukseen. EU:n tietosuoja-asetuksen 6. artiklassa on lueteltu henkilötietojen laillisen käsittelyn perusteet, joista vain yksi on siis suostumus.

Sopimussuhde ja henkilötietojen käsittely. Ryhtyessään asiakassuhteeseen henkilöstä eli rekisteröidystä tulee sopimusosapuoli, jonka henkilötietojen käsittely on tarpeen sopimuksen täytäntöön panemiseksi. Myös jo ennen sopimussuhteen syntymistä voidaan henkilötietoja käsitellä laillisesti, jos sopimuksen syntymistä edeltävien toimenpiteiden yhteydessä käsitellään henkilötietoja rekisteröitävän pyynnöstä (EU:n tietosuoja-asetuksen 6. artiklan 1. kohdan b alakohta) esimerkiksi tarjouksen tekemiseksi.

Myös työsuhde on sopimussuhde, jossa työntekijän ja työnhakijan henkilötietoja voidaan pääosin käsitellä laillisesti ilman erillistä työntekijän tai työnhakijan antamaa suostumusta. Toki lainsäädäntö (muun muassa EU:n tietosuoja-asetus ja laki yksityisyyden suojasta työelämässä 759/2004) tarkentaa, miltä tietosisältö- ja käsittelyosin suostumus on työntekijältä tarvittaessa saatava, mutta työsuhteen edellyttämien perustietojen käsittely perustuu pääosin sopimussuhteeseen ja EU:n tietosuoja-asetuksessa henkilötietojen käsittelyn lupaperusteeksi määriteltyyn oikeutettuun etuun.

Kun kyseessä on asiakas- tai työsuhteeseen perustuva sopimussuhde, voidaan sopimussuhteeseen ryhtymisen katsoa sisältävän rekisteröidyn suostumuksen niiden henkilötietojen osalta, jotka ovat välttämättömiä asiakas- tai työsuhteen hoitamisen kannalta. Sopimuksen syntyessä henkilötietojen rekisterinpitäjän tulee pystyä osoittamaan sen syntyminen yksiselitteisesti ja sopimussuhteen täyttämisen kannalta välttämättömät henkilötiedot.

Jos tarkastellaan puolestaan rekisteröidyn sellaisten henkilötietojen käsittelyä, jotka eivät ole välttämättömiä sopimussuhteen hoitamisen kannalta, kuten sopimussuhdetta laajemmat henkilötietojen käsittelyn tarkoitukset, tulee näiden henkilötietojen osalta saada pääsääntöisesti rekisteröidyn suostumus.

Rekisterinpitäjä voi kuitenkin omalta osaltaan asettaa sopimussuhteen syntymisen ehdoksi rekisterinpitäjän kulloinkin voimassa olevan julkisen, selkeän ja yksiselitteisen (esim. tietosuojaseloste) tietosuojakäytäntöjen hyväksymisen. Tällöin sopimussuhteen solmimista harkitsevan rekisteröitävän henkilön tulee niihin perehtyä ja hyväksyä ne viimeistään sopimuksen teon yhteydessä.

Hyväksymällä henkilötietojen tietosuojakäytännöt rekisteröity antaa rekisterinpitäjälle suostumuksen käyttää henkilötietojaan esimerkiksi sopimussuhdetta laajempiin henkilötietojen käsittelyn tarkoituksiin, kuten markkinointi- ja profilointitarkoituksiin. Rekisterinpitäjän tulee tällöin sopimussuhteen solmimisen yhteydessä huolehtia siitä, että rekisteröidyn hyväksyntä rekisterinpitäjän tietosuojakäytännöille on saatu yksiselitteisesti, yksilöidysti ja tietoisesti ja että tämä pystytään osoittamaan. Lisäksi rekisterinpitäjän tulee pystyä rajoittamaan henkilötietojen käsittelyä sopimussuhteen aikana, jos rekisteröity peruuttaa antamansa suostumuksensa kokonaan tai osittain.

Suostumuksen vapaaehtoisuuden vaatimuksen täyttymiseksi voidaan katsoa riittävän asiakas- tai työsuhdetta harkitsevan vapaan valinnan mahdollisuus sopimuskumppaninsa osalta. Jos rekisterinpitäjän voimassa oleva tietosuojakäytäntö ei mahdollista sopimuskumppania tyydytä, hän voi kieltäytyä sopimussuhteesta ja vaihtaa sopimuskumppania vapaasti.

Viranomainen ja henkilötietojen käsittely. Sankarin ja Wibergin artikkelissa viranomaisten oikeus henkilötietojen käsittelyyn on huomioitu mainitsemalla, että henkilötietojen käsittelyä määritteleviä lakeja on sosiaali- ja terveydenhuollossa sekä rikosasioissa, mutta julkisen vallan käyttöön liittyvää oikeutta henkilötietojen käsittelyssä ei ole artikkelissa sen tarkemmin huomioitu. Vaikka rekisteröidyn suostumus tietyissä tilanteissa tarvitaankin, artikkelin perusteella saa helposti sellaisen virheellisen käsityksen, että myös viranomainen tarvitsisi aina henkilötietojen käsittelyyn suostumuksen.

Suomessa viranomaisella ja yksityisellä toimijalla, jolle on siirretty viranomaistehtäviä, on julkisen vallan käyttöön liittyvä oikeus käsitellä rekisteröidyn henkilötietoja ilman rekisteröi-

dyn antamaa suostumusta. Tämä on yksiselitteisesti määritelty myös EU:n tietosuoja-asetuksen 6. artiklan 1. kohdan alakohdassa e. Viranomaisten toimintaa henkilötietojen käsittelyssä ja niiden luovuttamisessa säätelee lisäksi laaja joukko muita lakeja.

Tietosuojakäytännöt

Sankarin ja Wibergin artikkelissa on käytetty yhtenä tutkimuksen hypoteesina (H4) tietosuojakäytäntöjen yhdenmukaisuutta eri toimijoiden kesken. Tehdyn tutkimuksen perusteella todetaan, että tietosuojakäytännöt eivät ole yhdenmukaisia virastoissa ja yrityksissä eikä niiden kesken. Tätä pidetään artikkelissa asiana, joka pitäisi korjata.

Käytännössä tämä on mahdoton yhtälö, eikä sääntelykään tätä edellytä, kunhan vain noudatetaan EU:n tietosuoja-asetusta ja kansallista lainsäädäntöä, jotka asettavat säännöt henkilötietojen käsittelylle. Eri rekisterinpitäjät toteuttavat tietosuojaa näiden sääntöjen perusteella. Säännöt voivat hieman vaihdella esimerkiksi rekisterinpitäjän perusteella. Myös esimerkiksi se, miten rekisterinpitäjä teknisesti suojaa tietonsa, on rekisterinpitäjän päätettävissä. Olennaista on se, että rekisteröidyn tiedot suojataan lainsäädännön mukaisesti.

Lopuksi

Sankarin ja Wibergin artikkelissa on paljon hyvää tietoa EU:n tietosuoja-asetuksesta, sen soveltamisesta ja käytännön toimivuudesta. Tietosuojaan liittyvä sääntely on tänä päivänä erittäin tarpeellista sekä rekisteröidyille että rekisterinpitäjille heidän oikeusturvansa takia. Sääntelyn soveltaminen käytännössä on kuitenkin ollut haastavaa. Tietosuoja-asetuksen vaatimuksien täyttämisestä on tullut monelle organisaatiolle vaativa tehtävä, koska sitä on ryhdytty toteuttamaan turhankin monimutkaisesti.

Positiivisena asiana voidaan nähdä, että viime vuonna organisaatioissa tehtiin paljon tietosuojaan liittyviä kehitystoimenpiteitä, kun EU:n tietosuoja-asetuksen soveltaminen alkoi. Olemme samaa mieltä Sankarin ja Wibergin kanssa siitä, että vieläkin organisaatioissa on tehtävä työtä lainsäädännön vaatimusten asianmukaiseksi täyttämiseksi.

Tämän vuoden alusta Suomeen saatiin vihdoin ja viimein voimaan kansallinen tietosuojalaki, joten nyt meillä on toimivaltainen valvontaviranomainen. Tietosuojavaltuutetun toimistoon oli viime vuonna tullut jo yli tuhat ilmoitusta tietoturvaloukkauksista. EU:n tietosuoja-asetuksen mukaisia hallinnollisia sanktioita ei ole Suomessa vielä langetettu, kuten on asian laita muualla Euroopassa.

Esimerkiksi Ison-Britannian tietosuojaviranomainen (*Information Commissioner's Office*) määräsi Marriott-hotelliketjulle noin 110 miljoonan euron hallinnollisen sanktion. Syynä oli vuoden 2018 lopulla Marriottin varausjärjestelmästä löydetty tietoturva-aukko, jonka kautta paljastui noin 500 miljoonan asiakkaan henkilötietoja. Suomessa ensimmäiset hallinnolliset sanktiot on voitu määrätä vasta tämän vuoden elokuusta lähtien, kun toimintansa on aloittanut toimivaltuutta käyttävä tietosuojavaltuutetun toimiston kolmijäseninen kollegio.

Suomessa on viime vuosina korostettu lain vaikutusten arvioinnin tärkeyttä. Lainsäädännön ja toimenpideohjelmien vaikutusten arviointi on ollut kuitenkin vähäistä. Lainsäädännön toimivuuden parantamiseksi ja tehokkuuden lisäämiseksi tulisi oikeustieteellisessä tutkimuksessa lisätä empiirisen tiedon hyödyntämistä. Empiirisessä oikeustutkimuksessa selvitetään yhteiskunnan toimintamekanismeja eli lakien tosiasiallisia vaikutuksia ja niissä säädettyjen oikeuksien toteutumista, jotta näin saatua tietoa voidaan käyttää poliittisen päätöksenteon perustana lainsäädäntötyössä.

Sankarin ja Wibergin artikkeli on tärkeä avaus tietosuojan empiiriselle tutkimukselle Suomessa. Tietosuojaan liittyen olisikin tärkeää tutkia jatkossa sekä rekisterinpitäjien että valvontaviranomaisen näkemyksiä lakiuudistuksista, jotta voidaan monipuolisemmin selvittää nykyisen sääntelyn toimivuutta ja mahdollisten sääntelyhäiriöiden olemassaoloa.